

Military Operations

Command & Control Countermeasures (C2CM)

**Headquarters
Department of the Army
Washington, DC
31 July 1992**

Unclassified

SUMMARY of CHANGE

AR 525-20

Command & Control Countermeasures (C2CM)

This revision--

- o Establishes the basis for Army Command & Control Countermeasures Strategy implementation.
- o Specifies responsibilities for principle officials Headquarters, Department of Army and major army commands.
- o Changes Army C3CM policy to C2CM as found in Army doctrine FM 100-15.
- o Prescribes planning guidance for implementation of the C2CM strategy.
- o Provides guidelines for security classification and downgrading for C2CM planning.

Effective 31 August 1992

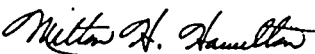
Military Operations

Command & Control Countermeasures (C2CM)

By Order of the Secretary of the Army:

GORDON R. SULLIVAN
General, United States Army
Chief of Staff

Official:


MILTON H. HAMILTON
Administrative Assistant to the
Secretary of the Army

History. This update printing publishes a revision of this publication. Because the publication has been extensively revised, the changed portions have not been highlighted.

Summary. This regulation implements assigned service tasks from JCS Memorandum of Policy No. 30. It sets forth Army policy for Command, and Control, Countermeasures, establishes responsibility for C2CM, incorporates revised definition of electronic warfare, clarifies C2CM terminology, and updates references and definitions. This regulation represents a significant change in

emphasis from joint C3CM policy while supporting its intent to achieve synergism from fire support, electronic warfare, deception and operations security.

Applicability. This regulation applies to the Active Army, U. S. Army Reserve, and Army National Guard.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff for Operations and Plans. The DCSOPS has the authority to approve exceptions to this regulation which are consistent with controlling law and regulation. The DCSOPS may delegate this authority in writing to a division chief within the proponent agency who holds the rank of colonel or the civilian equivalent. The approval authority will coordinate all questions regarding the scope of authority to approve exceptions with HQDA, OTJAG, ATTN: DAJA–AL, Washington, D.C. 20310–2200.

Army management control process. This regulation is not subject to the internal control procedures and requirements of AR 11–2 Internal Control Systems.

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior

approval from HQDA (DAMO–FDI), WASH, DC 20310–0460.

Interim changes. Interim changes to this regulation are not official unless authenticated by the Administrative Assistant to the Secretary of the Army. Users will destroy interim changes on their expiration dates if the changes are not superseded or rescinded earlier.

Suggested Improvements. The proponent agency of this regulation is the Office of the Deputy Chief of Staff for Operations and Plans. Users are invited to send comments and suggestions for improvement on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQDA (DAMO–FDI), WASH, DC 20310–0460.

Distribution. Distribution of this publication is made in accordance with the requirements of DA Form 12–09–E, block number 3517 intended for command level C for Active Army, USAR, and ARNG, less MDW, COE, HSC, and CID.

Contents (Listed by paragraph and page number)

Chapter 1

Introduction, page 1

Purpose • 1–1, page 1

References • 1–2, page 1

Explanation of abbreviations and terms • 1–3, page 1

C2CM versus command, control, and communications countermeasures (C3CM) • 1–4, page 1

General • 1–5, page 1

C2CM Strategy • 1–6, page 1

C2CM Program Objectives • 1–7, page 1

Army Goals for C2CM Strategy Implementation • 1–8, page 1

Chapter 2

Responsibilities, page 2

Section I

Principal Officials of Headquarters, Department of Army, page 2

Assistant Secretary of the Army, (Research Development and Acquisition (ASA (RDA))) • 2–1, page 2

The Deputy Chief of Staff for Operations and Plans (DCSOPS)

• 2–2, page 2

The Deputy Chief of Staff for Personnel (DCSPER) • 2–3, page 2

The Deputy Chief of Staff for Logistics (DCSLOG) • 2–4, page 2

The Deputy Chief of Staff for Intelligence (DCSINT) • 2–5, page 2

The Director of Information Systems for Command, Control, Communications, and Computers (DISC4) • 2–6, page 2

The Commander, United States Army Operational Test and Evaluation Command (OPTEC) • 2–7, page 3

Section II

Commanders of Major Army Commands, page 3

The Commanding General, United States Army Training and Doctrine Command (CG, TRADOC) • 2–8, page 3

The Commanding General, United States Army Materiel Command (CG, AMC) • 2–9, page 3

The Commanding General, United States Army Intelligence and Security Command (INSCOM) • 2–10, page 3

The Commanding General, United States Army Information Systems Command (CG, USAISC) • 2–11, page 3

* This publication supersedes AR 525–20, 1 July 1981.

Contents—Continued

The Commanders, Army tactical and operational level commands

- 2–12, *page 3*

Chapter 3

Strategy Implementation, *page 4*

General • 3–1, *page 4*

Planning Guidelines • 3–2, *page 4*

Specific intentions of C2CM planning • 3–3, *page 4*

Planning Authorities • 3–4, *page 5*

Security Classification Guidance • 3–5, *page 5*

Appendix A. References, *page 6*

Figure List

Figure 3–1:, *page 4*

Glossary

Index

Chapter 1 Introduction

1-1. Purpose

This regulation defines C2CM, describes its role in combat operations, identifies objectives, prescribes policy, and assigns responsibilities.

1-2. References

Required and related publications are listed in Appendix A.

1-3. Explanation of abbreviations and terms

Abbreviations and terms used in this regulation are explained in the glossary.

1-4. C2CM versus command, control, and communications countermeasures (C3CM)

Modern military communications are important to the timely execution and coordination of battlefield operations. Communications are not the focus of the Army C2CM strategy whereas command and control targets are the focus using direct and indirect means to deny, disrupt, degrade, and destroy. Influencing the enemies command and control functions can delay or deny the proper concentration of combat power. Command and control functions are performed through an arrangement of personnel, equipment, facilities, and procedures employed by the commander in planning, directing, coordinating, and controlling forces to accomplish the mission. Therefore, the C2CM strategy attacks and influences the C2 means to gather intelligence, assess options, formulate plans, and issue or execute orders. Communications are one means to maintain C2 of forces, weapons, and battlefield functions.

1-5. General

a. US Army commanders will employ appropriate assets to counter enemy C2 and to protect friendly C2 from similar enemy activities with direct and indirect measures. The means by which C2 and counter C2 measures are employed vary and encompass several battlefield operating systems (BOS) and functions.

b. Resources to support the C2CM concept are found throughout the force. These resources include, but are not limited to, destruction (Fire Support), electronic warfare (EW), military deception, intelligence, counterintelligence, operations security, special operations, and other military activities.

c. Knowledge of critical nodes (see glossary), as associated with high value target (HVT), and key connectivity links in the enemy and friendly C2 systems are essential to the planning and execution of US and allied C2CM. The Joint Command HVT list is a Joint Staff responsibility in coordination with component commands. Assistance in developing this list is available through the Defense Intelligence Agency (DIA) Tailored Analytical Intelligence Support to Individual EW program and Command, Control, Communications and Countermeasures (C3CM) Projects (TASIP) program. Doctrinal combat/integrating developers at the Combined Arms Center (CAC) and service schools produce HVT lists during the system threat assessment process.

d. Intelligence and threat analysis support is required for optimum C2CM planning, system development, and operations. Operational commanders must weigh the advantages to be gained by countering enemy C2 nodes against the potential loss of intelligence from intercepted enemy emissions—particularly those from higher command echelons—and the need to protect intelligence sources and methods.

1-6. C2CM Strategy

C2CM is the integrated use of lethal and non-lethal means, OPSEC, and military deception against the enemy's command and control (C2) capabilities. Integration of C2CM denies effective execution of plans and orders by the enemy, impedes or denies accomplishment of military objectives, and conserves friendly combat resources. The resulting outcome is to cause the enemy commander to reassess combat plans and intentions.

a. A military force that builds a C2CM capability with proper training and resources will pose a very serious threat to an enemy commander's ability to execute successful combat operations. Degradation of electronic surveillance and target acquisition capabilities help prevent the effective deployment of combat forces and accurate employment of combat weapons. Disruption of C2 means will deny the ability to recover quickly from battle attacks or effective exploitation by maneuvering units. The presentation of false data to intelligence elements will cause confusion in the allocation of combat elements and prevent effective employment of these resources during critical combat engagements. Destruction of key facilities, command posts, and weapon control points will seriously influence the outcome of combat operations. In essence, C2CMs deny, degrade, disrupt, or destroy the complete use of key C2 capabilities.

(1) Direct Measures (see terms, glossary) counter the enemy commander's means of controlling battlefield functions, using both lethal and non-lethal attack capabilities against troop control centers and means, weapon systems control centers and fire direction means, reconnaissance systems, and force command planning centers, including commanders and their staffs. Direct measures deny effective use of the means for C2.

(2) Indirect Measures (see terms, glossary) protect friendly command and control from both friendly and adversary actions. These measures include OPSEC and military deception and are used to deny accurate and timely information about friendly forces or present false information about those forces. Electronic Protection Measures (EPM) and tactics will reduce or eliminate the effects of hostile attempts to degrade or disrupt friendly C3. Emission control (EMCON) is critical to ECCM (EPM-NATO) planning as a protective measure.

b. Electronic deception and the use of Wartime Reserves Modes (WARM) can play an important role in the execution of direct and indirect C2 measures. By altering friendly stereotyped electromagnetic profiles and eliminating or disguising telltale control procedures or network interrelationships, the capability of opposing commanders to select the most rewarding C2 targets can be significantly reduced. By presenting notional targets to mislead, decoy, or disguise friendly capability or intentions, electronic deception can influence opposing commanders to making decisions which are advantageous to friendly forces. The use of WARM by attacking forces can significantly reduce electronic detection and enhance deception.

1-7. C2CM Program Objectives

C2CM objectives are as follows:

a. Maximize U.S. capabilities to—

(1) Deny hostile military commanders the ability to command and control their forces effectively.

(2) Protect friendly C2 resources from enemy attempts to disrupt, degrade, detect, or destroy them.

b. Develop C2CM capabilities that are interoperable, compatible, and mutually supportive in joint and combined operations.

c. Integrate C2CM into military plans, operations, and exercises to maximize U.S. and allied military effectiveness.

d. Train or familiarize personnel at all levels with C2CM activities and objectives.

e. Evaluate the effects of C2CM on friendly and hostile C3.

1-8. Army Goals for C2CM Strategy Implementation

a. To maintain the proficiency of forces and develop capabilities to employ C2CM across the operational continuum.

b. To employ C2CM at all times to maximize C2 effectiveness and degrade the opposing force C2 effectiveness.

c. To coordinate C2CM programs, tactics, and concepts with appropriate DOD agencies/departments and, when appropriate, with allied nations.

d. To have U.S. Army C2CM procedures and materiel programs respond to operational missions and objectives of CINCs and Army MACOMs. This will be done to complement the effects of other weapon systems and effectively support the combat efforts of the United States and its allies.

e. Interoperability with USAF, USN and USMC C2 systems with a planned, step-by-step procedure. It will be aimed toward achieving a capability that satisfies joint and combined needs as well as individual US Army requirements.

f. To test all fielded systems that may be affected by hostile C2CM in C2CM environment that quantitatively and qualitatively represents the expected threat, described in the system STAR and reflected in the TTSP.

g. To develop smart munitions, deception devices, antiradiation weapons, targeting systems and other materiel having C2CM potential; and test these systems capabilities against representative or expected threat targets described in the STAR and reflected in the TTSP.

h. To engineer C2 countermeasures using US countermeasures equipment, materiel, and procedures. This includes built-in OPSEC measures to protect against foreign intelligence collection with additional counter intelligence/security, as required by DOD/Army security guidelines policy.

i. US Army Operational Requirement Documents (ORDs), Mission Equipment Needs Statements (MENS), Operational Needs Statements (ONS) and the subsequent development, design, and test of systems will consider and incorporate, where appropriate, capabilities to support the C2CM strategy implementation (lethal, non-lethal, OPSEC, or deception). These documents and acquisition activities will also evaluate the potential for unintentional interference with US and allied systems and take into account electromagnetic environmental effects (E3).

j. C2CM training will be a standing objective in all major Army exercises. During specified portions of the exercises, C2CM will be given priority over other exercise objectives.

k. To provide US Army intelligence element support to C2CM planners and commanders at all echelons for planning and conducting C2CM. These elements will assist in preparing scenarios which represent anticipated threats and targets; they will also provide critical node analysis to aid in developing C2CM plans, tactics, and asset capabilities. Anticipated threats and targets are described in the STAR per AR 381-11.

l. To eliminate or minimize vulnerability to friendly C2CM systems and equipment under development through shared responsibility involving the proponent, combat developer, materiel developer, and user.

Chapter 2 Responsibilities

Section I

Principal Officials of Headquarters, Department of Army

2-1. Assistant Secretary of the Army, (Research Development and Acquisition (ASA (RDA)))

ASA(RDA) will—

a. Assume responsibility for the research, development, test, and evaluation (RDTE) required to support C2CM capabilities.

b. Be responsible for acquisition and life-cycle management of materiel in support of the C2CM strategy.

c. Plan and coordinate development or procurement of simulated hostile C2CM systems for testing and training.

d. Conduct research and acquire basic knowledge of the techniques and circuitry required to provide an effective defensive C2CM capability in appropriate types of Army equipment and ensure Program Executive Officers use this knowledge.

2-2. The Deputy Chief of Staff for Operations and Plans (DCSOPS)

The DCSOPS will—

a. Serve as HQDA POC for C2CM and coordinate Army C2CM functions.

b. Supervise and determine the C2CM forces readiness and

C2CM operational capabilities of Army forces to accomplish assigned missions under real or assumed conditions.

c. Supervise the integration of C2CM into Army force strategies modernization, and unit training.

d. Provided for force integration of systems support of the C2CM strategy.

e. Develop Army C2CM policy, programs, and validate force structure requirements for units of the Active Army, US Army Reserve, and Army National Guard.

f. Provide DA Staff supervision of the planning, execution, and evaluation of C2CM in the fielding training exercises.

g. Validate, coordinate, and approve materiel requirements documentation and establish priorities to support C2CM.

h. Provide DA Staff supervision of operational testing of equipment, systems, and organizations in support of the C2CM strategy.

i. Assess C2CM interoperability with the other Services and allies and make recommendations for improvements.

j. Coordinate C2CM matters with the other military services and allies, as appropriate.

k. Develop policies and programs for individual C2CM strategy training at Army, Joint, Combined, and National Defense University schools.

2-3. The Deputy Chief of Staff for Personnel (DCSPER)

The DCSPER will—

a. Ensure proper assignment and management of soldiers to key C2CM staff positions

b. Ensure the inclusion of C2CM training courses in the Army Training Resources and Requirements System (ATRRS).

2-4. The Deputy Chief of Staff for Logistics (DCSLOG)

The DCSLOG will—

a. Ensure logistical support for C2CM concept materiel within DCSLOG assigned functions.

b. Ensure proper provisions for C2CM concept materiel under the Integrated Logistic Support Program during the materiel acquisition process.

c. Provide continuous logistic support for fielded C2CM materiel and test equipment.

d. Coordinate all requests for foreign materiel sales (FMS) involving C2CM equipment (EW, Fire Support, OPSEC, Deception) with ODCSOPS (DAMO-FDI) and applicable Army agencies.

2-5. The Deputy Chief of Staff for Intelligence (DCSINT)

The DCSINT will—

a. Provide intelligence support to MACOM C2CM planning requests as stated under DIA request procedures for Tailored Analytical Intelligence Support to Individual EW and C3CM Projects (TASIP).

b. Ensure C2CM threat information is produced to support materiel, training, doctrinal and operational needs of Army agencies and commands.

c. Monitor and coordinate the production aspects of threat C2CM for transmittal to materiel/combat developers and MACOMs.

d. Serve as the proponent for Information System Security (ISS). (AR 380-19).

e. Ensure adequate availability of foreign equipment for test, exploitation and susceptibility study.

2-6. The Director of Information Systems for Command, Control, Communications, and Computers (DISC4)

The DISC4 will—

a. Exercise responsibility for automated systems, electromagnetic spectrum management, and the automation/ communications management aspects of C2CM.

b. Ensure C2CM combined interoperability requirements are addressed and satisfied with mission area agreements of US and allied forces such as NATO and the American, British, Canadian, Australian (ABCA) Armies Standardization Program.

c. Ensure software compatibility with appropriate joint combined and allied forces.

d. Coordinate with ODCSINT concerning the management and implementation of an ISS program in support of C2CM policy.

2-7. The Commander, United States Army Operational Test and Evaluation Command (OPTEC)

The Commander, OPTEC will—

a. Ensure objectives are incorporated into Test Design Plans to evaluate equipment performance in direct and indirect C2CM roles.

b. Ensure operational tests adequately stress equipment in a well simulated hostile threat C2 countermeasures environment.

(1) Exercise responsibility for the specific operational testing of C-E/and related systems, (includes RF/IR/EO defensive/offensive systems) in a C2CM threat environment.

(2) Conduct operational tests on assigned major and Category 1, non-major C-E/and related systems in an environment that represents the hostile C2CM threat.

(3) Provide policy guidance, review, and approve, as appropriate, plans and other documents relating to U.S. Army (including Joint programs) testing in a C2CM hostile threat environment conducted by other designated testers for Categories 2 through 4 non-major C-E/and related systems.

Section II

Commanders of Major Army Commands

2-8. The Commanding General, United States Army Training and Doctrine Command (CG, TRADOC)

The CG, TRADOC will—

a. Develop and test organizational and operational concepts and doctrine on the tactical and technical employment of C2CM to support Army operations in the field.

b. Recommend Science and Technology Objectives (STO) for C2CM to DA.

c. Prepare and provide recommendations on establishing, revising, or eliminating Required Operational Capability (ROC) documentation for C2CM operations by the Army.

d. Program for and conduct troop tests that may be required in coordination with OPTEC.

e. Direct and supervise the preparation of training literature and the training of personnel in the use, operation, and maintenance of C2CM strategy equipment to be used by Army units.

f. Integrate C2CM strategy training into TRADOC school curricula.

g. Integrate requirements and procedures for countering hostile C2CM threat in combat developments and training activities.

h. Recommend establishment, revision, or elimination of Training Device Requirements (TDR) related to the C2CM strategy.

i. Develop doctrine, Tactics, Techniques, and Procedures (TTP) to support the C2CM strategy and program an objective implementation using a MACOM HVT lists as a baseline.

j. Review requirements for decision aids that automate the C2CM strategy planning functions and initiate action under the Concept Based Requirements Systems (CBRS) to field their capability to tactical units.

k. Coordinate or provide U.S. representation to various allied or joint C2CM doctrinal and combat development fora.

2-9. The Commanding General, United States Army Materiel Command (CG, AMC)

The CG, AMC will—

a. Perform materiel RDTE, procurement, storage, depot maintenance, and distribute materiel to the force as assigned by DA in support of the C2CM concept.

b. Ensure logistical support of all C2CM systems in the Integrated Logistic Support Program.

c. Prepare technical literature for the operation and maintenance of equipment in a C2CM environment in coordination with Program Executive Officer procurement programs.

d. Incorporate the most cost-effective anti-jamming circuitry and

other C2 protection features into susceptible communications-electronic equipment and recommend trade-offs to the combat developer.

e. Conduct C2CM vulnerability developmental tests and studies on equipment/systems and foreign C-E equipment.

f. Provide support and assistance, as required, to other army commands and Program Executive Officers in fulfilling their assigned C2CM vulnerability responsibilities.

g. Develop and procure simulated C2CM systems, as required, when requested.

2-10. The Commanding General, United States Army Intelligence and Security Command (INSCOM)

The CG, INSCOM will—

a. Support Army MACOM C2CM strategy activities in exercises, tests, and experiments to include assistance in assessing the effectiveness of applied C2CM.

b. Recommend changes or additions to CG, TRADOC, for C2CM concepts, doctrine, and related matters at the echelons above corps, joint, and combined levels.

c. As requested by CG, TRADOC, take part in combat development studies, experiments, and tests of organizational and operational concepts and doctrine.

d. Provide support and assistance to other Army commands in determining their C2CM vulnerabilities and assessing threat susceptibilities.

e. Recommend Science and Technology Objectives (STO) for C2CM to HQDA.

f. Perform C2CM materiel acquisition functions assigned by DA for EAC INSCOM forces.

g. Appoint a staff point of contact to assist operational planners with C2CM strategy implementation.

2-11. The Commanding General, United States Army Information Systems Command (CG, USAISC)

The CG, USAISC will—

a. Develop, test, and recommend to CG, TRADOC, organizational and operational concepts and doctrine; these concepts and doctrine pertain to the employment of C2CM to support the operations of the Army portion of the Defense Communications System, Army air traffic control facilities, and USAISC-operated facilities in echelons above corps (EAC).

b. Integrate requirements and procedures for countering hostile C2CM threat in combat developments and training activities.

c. Prepare literature pertaining to operation of mission-peculiar equipment in a hostile C2CM threat environment.

d. Assist the CG, AMC, in determining the C2CM and antiradiation missile vulnerabilities of USAISC systems and, as appropriate, conduct C2CM susceptibility studies, vulnerability tests, and on mission-peculiar equipment/systems.

2-12. The Commanders, Army tactical and operational level commands

These Commanders will—

a. Exercise operational control over all C2CM strategy resources assigned.

b. Maintain C2CM readiness for Army forces assigned.

c. Integrate C2CM training into unit training programs, maneuvers, and exercises, as appropriate.

d. Recommend to CG, TRADOC changes or additions to C2CM concept, doctrine, tactics, or techniques that may result from the evaluation of training prescribed in (C) above.

e. Designate a single staff component (DCSOPS/G-3) at headquarters staffs level to serve as a focal point for C2CM strategy implementation.

f. Identify operational and intelligence requirements, conduct evaluations, and request equipment needed to attain the required C2CM posture in consonance with other known requirements and priorities.

g. Identify personnel requirements and qualification for C2CM

activities; train and provide personnel to subordinate operational commands.

h. Ensure command and control capabilities are adequate to support planning and implementation of the C2CM strategy.

i. Maintain personnel security programs and provide guards and other defensive forces to protect against sabotage and attack of command and control facilities.

j. Develop and maintain a capability to perform military deception. This includes Battlefield Deception support to operational plans (AR 525–21).

k. Exercise commanders, staffs, and the intelligence system ability to support C2CM planning and implementation in order to gain experience in the detection of hostile countermeasure nodes.

l. Evaluate the capability of US Army combat forces to perform both offensively and defensively in an environment representative of hostile countermeasure nodes.

Chapter 3 Strategy Implementation

3–1. General

Modern military forces are highly dependent on C2 for effective application of combat power. The fundamental elements of C2 are personnel, facilities, sensors, processors, and decision making. Army doctrine frequently refers to these elements in a decide, detect, and deliver methodology for attacking enemy forces, facilities, and high value target systems that may interfere with successful mission accomplishment.

a. Targets. Targets are identified in terms of what, when, and where enemy capabilities pose the greatest potential to interfere with the success of friendly operations. Priority must first go to dealing with the most threatening enemy means within three basic target sets: (1) follow-on maneuver; (2) command, control, and communications (C3); and (3) high value targets.

b. Old method. Historically, the targeting methodology of detecting enemy targets; deciding whether, when, and how to attack them; and then delivering attacks against them is reactive and does little to wrest the initiative from the enemy or shape the future close fight. Such reactive procedures create high stress on the performance of sensors, processors, C2, decision makers, communications, and attack means because they force operations into a compressed time frame. In addition, this technique is frequently not responsive enough in a highly mobile situation.

c. New method. The decide, detect, and deliver planning process is focused by combining it with forward thinking to provide the basic framework for battlefield planning in a Tactical Operations Center (TOC) or theater army operations center. This methodology is key to the effective use of fire, maneuver, and C2CM strategy implementation in military operations. Forward thinking protects friendly operations, orients the proactive planning process to identify relevant targets, and provides the method to determine target specifics, such as—times when the target is likely to be active, detected, and attacked with the required resources.

3–2. Planning Guidelines

The planning process begins with the receipt of a mission (assigned from Echelons-Above-Corps (EAC) or delivered internally). The focus is on coordinating and synchronizing the activities of the functional planning cells to accomplish the planning mission within the commander's intent and guidance.

a. The Commander and staff have the responsibility to ensure all activities are synchronized in time and space. The G–3 planning element is responsible for coordinating activities and must ensure that maneuver, aviation, and C2CM elements interact effectively and cooperate with elements at EAC. G–3 planners deconflict fire support, deception, electronic warfare, and OPSEC plans to ensure economy of fires and to provide the commander with multiple options.

b. It is the responsibility of the G–3 planning element to write the operations orders and coordinate with each functional planning cell regarding the specific tasks. Most importantly, the G–3 planning element ensures that the operations plans are written based on the guidance and direction provided by the commander regarding use of countermeasures. Rules of Engagement (ROE) must be clearly understood as received from higher level commanders or clarified if not understood.

3–3. Specific intentions of C2CM planning

Effective C2CM can deny the enemy commander the means required to concentrate the combat power of forces. Fires at depth against follow-on combat forces, command posts (CPs) and weapons control centers can significantly disrupt enemy tempo. Lethal and non-lethal attack can be used in conjunction with deception and OPSEC or in support of offensive deep maneuver or counterattacks. (See Figure 3–1)

a. Attack of enemy target acquisition, intelligence gathering, and C2 systems is conducted through a combination of lethal and non-lethal attacks and the use of indirect OPSEC and deception means. Normally, attacks using electromagnetic applications are conducted by radio frequency (RF), infrared (IR) or electro-optical (EO) means with results of damage, destruction, or disruption (non-lethal) to susceptible targets. The object of these actions may not be to completely destroy the enemy C2 system, but rather to create ambiguity, and to interrupt his ability to make timely, correct decisions, and transmit plans or orders.

b. An operational maneuver may be supported by fires of both surface-to-surface and air-to-surface systems, including both Air Force and Army aviation. On a time schedule dictated by that of the battle, identified targets that advantageously influence the friendly operation (HVT) are engaged with direct C2CM means (fires – EW). Attack systems are matched to the target set, and targets are engaged to delay, disrupt, damage or destroy them. Additionally, C2 facilities are attacked during the time when an enemy is attempting to react to friendly maneuver. Air Force EW and fire support should be coordinated through the battlefield coordination element/tactical air control center (BCE/TACC).

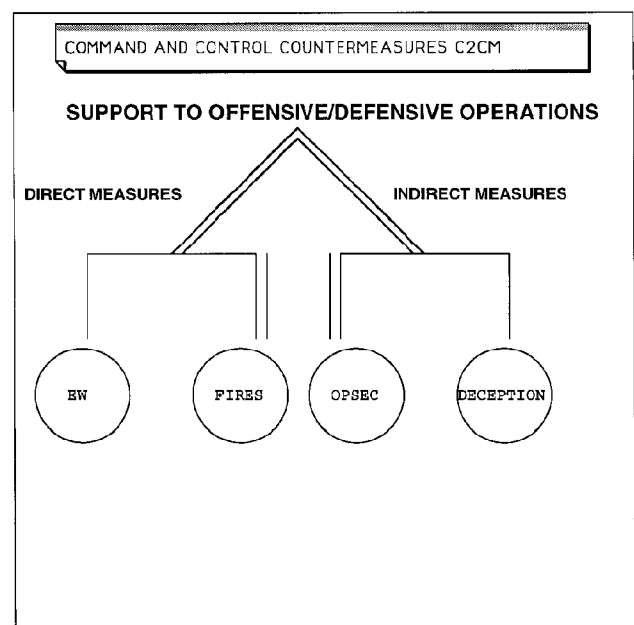


Figure 3-1.

c. C2CM in low intensity conflict (LIC) uses the same decide, detect, and deliver planning methodology. C2CM has applicability in all four categories of LIC; Contingency operations, Combatting terrorism, Insurgency/counterinsurgency, and Peacekeeping operations. Targeting of national infrastructure and unconventional threat

organizational structure with C2CM in consonance with the political, economic, and informational elements of national power is extremely important to US Army operations in LIC. These LIC targets are analogous to tactical HVT lists in conventional war involving armies with established doctrine and large force structures, but with the added dimension of being more amorphous in nature.

3-4. Planning Authorities

C2CM planning will be conducted in accordance with the references at Appendix A (References), Section I (Related Publications).

3-5. Security Classification Guidance

Information related to C2CM will be classified, downgraded, and declassified IAW AR 380-5. The following guidelines will generally apply:

a. The following information is UNCLASSIFIED:

(1) General C2CM policy, doctrine, strategies, tactics concepts, training programs, and new capabilities applicable to C2CM strategies being developed.

(2) Assignment of responsibilities for C2CM.

(3) C2CM involving the coordination of individual techniques or disciplines such as EW; battlefield deception; intelligence support; OPSEC; the use of such lethal/nonlethal means as artillery, air-delivered weapons, missiles, and conventional or special operations forces.

(4) US Army intentions to employ specific methods, procedures, and capabilities to protect its C2 from foreign counter-C2.

(5) Revelation of general US policy concerning the planning and conduct of service, joint, and combined C2CM or C3CM.

b. The following is CLASSIFIED as indicated:

(1) Information that reveals the extent and readiness of the United States to conduct C2CM will be classified SECRET. This information may be classified TOP SECRET if it reveals serious deficiencies of long-lasting duration or deficiencies reflecting the capability of a strategic force to accomplish its mission. Downgrade: Originating Agency Determination Required (OADR)

(2) Concepts, equipment, or techniques applicable to C2CM that reveal details of intelligence support to specific missions will be classified according to intelligence information and should be sanitized in accordance with current regulations to:

(a) Permit its handling at no higher than the SECRET level with noncompartmented access.

(b) Make it releasable to allies. Downgrade: OADR

(3) Information related to special techniques or equipment for C2CM will be classified on a case-by-case basis by the responsible agency or command, using guidelines in DOD directives 5200.1 and 5205.2 and supporting Army Regulations. Downgrade: OADR

(4) Joint C2CM guidance may be revealed to foreign nations authorized to have access to the level of classification and type of information involved when necessary for combined training, planning, or employment for C2CM. Downgrade as required by foreign disclosure policy or OADR.

Appendix A References

Section I Required Publications

DOD 5200.1

DOD Information Security Program (paragraph 2-5b(3))

DOD 5205.2

DOD Operations Security Program (paragraph 2-5b(3))

Section II Related Publications

AR 11-2

Internal Management Control

AR 25-1

The Army Information Resources Management Program

AR 70-1

System Acquisition Policy and Procedures

AR 71-1

Army Combat Developments

AR 71-9

Material Objectives and Requirements

AR 73-3

User Testing

AR 105-2

Electronic Counter-Countermeasures (ECCM) Electronic Warfare Susceptibility and Vulnerability

AR 105-3

Reporting Meaconing, Intrusion, Jamming and Interference of Electromagnetic Systems

AR 105-5

Electromagnetic Cover and Deception (EC&D)

AR 380-19

Information System Security

AR 381-11 (C)

Threat Support to US Army Force, Combat and Material Development

AR 525-21

Battlefield Deception Policy

AR 525-22

Electronic Warfare

AR 530-1

Operations Security

AR 530-2

Communication Security

DDB-2611-1-89 (DIA)

Procedures for Requesting Tailored Analytical Intelligence Support to Individual EW and C3CM Projects (TASIP)

DDB-1730-72-91 (DIA)

Joint Procedures for Intelligence Support to Electronic Warfare Reprogramming

MOP-6

Joint Chief Of Staff Memorandum Of Policy – 6, Electronic Warfare Policy

MOP-25

Wartime Reserve Modes Policy

MOP-30

Joint Chief of Staff Memorandum Of Policy - 30, Command, Control, and Communications Countermeasures Policy

MOP-116

Military Deception

FM 6-20

Fire Support in Combined Arms Operations

FM 11-50

Combat Communications within the Division

FM 34-1

Division Intelligence and Electronic Warfare Operations

FM 90-2

Battlefield Deception

FM 100-5

Operations

FM 100-15

Corps Operations (S)

MJCS 158-89

Procedures for Requesting Tailored Analytical Intelligence Support to Individual EW C2CM Projects (TASIP)

Section III Referenced Forms

This section contains no entries.

Section IV Prescribed Forms

This section contains no entries.

Glossary

Section I Abbreviations

ABCA

American, British, Canadian, Australian

AMC

US Army Materiel Command

ASA(RDA)

Assistant Secretary of the Army (Research, Development and Acquisition)

ARNG

Army National Guard

BCE

Battlefield Coordination Element

BOS

Battlefield Operating Systems

CAC

Combined Army Center

CG

Commanding General

CID

Criminal Investigative Division

COE

Chief of Engineers

CPs

Command Posts

C2

Command and Control

C2CM

Command, and Control Countermeasures

C3

Command, Control, and Communications

C3CM

Command, Control, and Communications Countermeasures

DA

Department of the Army

DCSINT

Deputy Chief of Staff Intelligence

DCSLOG

Deputy Chief of Staff for Logistics

DCSOPS

Deputy Chief of Staff for Operations and Plans

DCSPER

Deputy Chief of Staff for Personnel

DIA

Defense Intelligence Agency

DISC4

Director of Information Systems for Command, Control Communications, and Computers

EAC

Echelons-Above-Corps

ECCM

Electronic Counter-Countermeasures

EC&D

Electromagnetic Cover and Deception

EO

Electro-optic

EPM

Electronic Protective Measures

EW

Electronic Warfare

HQDA

Headquarters Department of the Army

HSC

Health Services Command

HVT

High Value Target

INSCOM

US Army Intelligence and Security Command

IR

Infrared

MACOM(s)

Major Army Command

MED

Manipulative Electronic Deception

MND

Mission Needs Document

MOP

Memorandum of Policy

NATO

North Atlantic Treaty Organization

ONS

Operational Needs Statement

OPSEC

Operational Security

OPTEC

US Army Operational Test and Evaluation Command

ORD

Operational Requirements Document

QRC

Quick Reaction Capability

RDTE

Research, Development, Test, and Evaluation

RF

Radio Frequency

ROC

Required Operational Capability

ROE

Rules of Engagement

STAR

System Threat Assessment Report

STO

Science and Technology Objective

TACC

Tactical Air Control Center

TASIP

Tailored Analytical Intelligence Support to Individual Projects

TDR

Training Device Requirement

TOC

Tactical Operations Center

TRADOC

US Army Training and Doctrine Command

TTP

Tactics, Techniques, and Procedures

US

United States

USAR

US Army Reserve

USACC

US Army Communications Command

USAISC

US Army Information Systems Command

WARM

Wartime Reserve Mode

Section II Terms

Command and Control Countermeasures (C2CM)

The integrated use of lethal and nonlethal means, OPSEC, and military deception against the enemy's command and control capabilities to deny him the ability to effectively execute plans and orders. C2CM is both direct and indirect. Direct measures counter the enemy commander's means of controlling battlefield functions, using both lethal and non-lethal attack capabilities against troop control centers and means, weapons systems control centers and fire direction means, reconnaissance systems, and force command planning means, including commanders and their staff. Direct measures deny the enemy commander the effective use

of his means of control. Indirect measures protect friendly command and control from both friendly and adversary actions. These measures include OPSEC and military deception and are used to deny the enemy commander accurate and timely information about friendly forces and to present the enemy false information about those forces.

Command and Control (C2)

The exercise of authority and direction by a properly designated commander over assigned or attached forces in the accomplishment of the mission. C2 functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating and controlling forces and operations in the accomplishment of the mission. (JCS Pub 1-02) Command, Control, and Communication Countermeasures (C3CM) The integrated use of operation security, military deception, jamming, and physical destruction, supported by intelligence, to deny information to, influence, degrade, or destroy adversary command, control, and communications (C3) capabilities and to protect friendly C3 against such actions. (JCS Pub 1-02)

Critical Node

Point in a C2 network whose disruption or destruction immediately degrades the ability of a force commander and staff to effectively command and control combat operations.

Battlefield Deception

Those operations or measures conducted at echelon theater and below to purposely mislead enemy forces by distorting, concealing, or falsifying indicators of friendly intent. (AR 525-21)

Electronic Warfare (EW)

Military action involving the use of electromagnetic energy to determine, exploit, reduce or prevent hostile use of the electromagnetic spectrum through damage, destruction, and disruption, while retaining friendly use of the electromagnetic spectrum. (AR 525-22) (JCS MOP6)

Electronic Protective Measures (EPM) (NATO)

That division of EW involving actions taken to ensure friendly effective use of the electromagnetic spectrum despite the enemy's use of electronic energy. There are two subdivisions of EPM:

Active EPM.

Detectable measure, such as altering transmitter parameters as necessary, to ensure friendly effective use of the electromagnetic spectrum.

Passive EPM.

Undetectable measures, such as operating

procedures and technical features of equipment, which are meant to ensure friendly effective use of the electromagnetic spectrum. (MC 64/6) C2CM Major Components

Direct measures

Those offensive measures taken to deny adversary decision makers the ability to effectively command and control their forces. (Generally applied with fire support and electronic warfare means)

Indirect measures

Those defensive measures taken to maintain effective C2 capabilities of friendly forces from actual or potential adversary counter C2. (Generally applied with operations security, and battlefield deception, or WARM means)

Operation Security (OPSEC)

A process of analyzing friendly actions in military operations and other activities to: (1) Identify those actions that can be observed by adversary intelligence systems. (2) Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. (3) Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

Military Deception

Actions executed to mislead foreign decision makers, causing them to derive and accept desired appreciations of military capabilities, intentions, operations, or other activities that evoke foreign actions that contribute to the originator's objectives. (JCS Pub 1-02)

Strategy

The art and science of developing and using political, economic, psychological, and military forces as necessary during peace and war, to afford the maximum support to policies, in order to increase the probabilities and favorable consequences of victory and to lessen the chances of defeat. (JCS Pub 1-02)

Wartime Reserve Mode

WARM are characteristics and operating procedures of sensor, communications, navigation aids, threat recognition, weapons, and countermeasures systems that (a) will contribute to military effectiveness if unknown to or misunderstood by opposing commanders before they are used, but (b) could be exploited or neutralized if known in advance. WARM are deliberately held in reserve for wartime or emergency use and seldom, if ever, applied or intercepted prior to such use. (JCS Pub 1-02)

Section III

Special Abbreviations and Terms

This section contains no entries.

Index

ASARDA, 2–1

C2CM

Objectives, 1–7

Goals, 1–8

Strategy Implementation, 1–8, 3–1

Planning Guidelines, 3–2, 3–3

Command, Control and Communications

Countermeasures, 1–4, 1–5c, app a,
3–5a(5)

DCSOPS, 2–2

DISC4, 2–6

DCSINT, 2–5

DCSLOG, 2–4

DCSPER, 2–3

Decide, Detect, Deliver Methodology, 3–1c

Direct Measures, 1–6a(1)

Electronic Deception, 1–6b

G–3 Staff, 3–2a, 3–2b, 2–12e

High value targets, 1–5c, 3–3b, 2–8i

Indirect measures, 1–6a(2)

Low Intensity Conflict, 3–3c

Major Army Commands, 2–8

Operation Security, 1–5b, 1–8h, 3–3, app a

Rules of Engagement, 3–2b

Security Classification Guidance, 3–5

Smart Munitions, 1–8g

Tactics, Techniques and Procedures, 2–8i

**Tailored Analytical Intelligence Support to
Individual EW, C3CM Projects, 1–5c,
app a, 2–5a**

Wartime Reserve Modes, 1–6b

Unclassified

PIN 049349-000

USAPA

ELECTRONIC PUBLISHING SYSTEM
TEXT FORMATTER ... Version 2.45

PIN: 049349-000

DATE: 11-24-98

TIME: 11:57:21

PAGES SET: 13

DATA FILE: a17.fil

DOCUMENT: AR 525-20

DOC STATUS: NEW PUBLICATION